UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,622	12/19/2001	Kenneth W. Aull	NG(MS)7194	2941

26294 7590 10/06/2006

TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVEVLAND, OH 44114

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/027,622	AULL ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to currently amended claim 8 and previously presented claims 1-7 & 9-16 filed 9/8/2006 have been fully considered but are not persuasive. The Examiner would like to point out that this action is final (See MPEP 706.07(a)).

Response to Arguments

Applicants contend that "nothing in Geer teaches or suggests that the authorization certificate is downloaded to a smart card." Examiner respectfully disagrees. Geer teaches that an authorized computer sends an authorized certificate to the smartcard , i.e. downloading and authorization certificate to the smartcard, in col. 6, lines 5-28. Furthermore, Geer teaches that the private key may be downloaded to the smartcard by the manufacturer or any other trusted source (col. 2, lines 40-50). Therefore, Geer discloses downloading a certificate and an associated private key to a token.

Applicants further contend that combination of Geer and Kanevsky "does not teach or suggest that a certificate and an associated private key are wrapped with a public key associated with the token ID." Examiner respectfully disagrees. In one of the embodiments disclosed, Geer teaches that during a transaction with another entity (an electronic merchant in this example) the client finds the need to authenticate the entity that he/she is communicating with to carry out the transaction where the merchant sends a certificate with the private key for the communications (col. 4, lines 2-9). However, since Geer did not explicitly disclose various elements, including that the certificate and the private key are wrapped by a public key associated with the token ID.

Therefore, for that element, Kanevsky was used to modify the transaction from Geer to be that of a password renewing transaction, where a client most definitely needs to authenticate himself/herself as well as to receive some way of authenticating the computer from which it requested the transaction (col. 8, lines 29-46). Furthermore, Kanevsky suggests the use of the public key and certificate (which are both associated with the token ID, i.e. the specific smartcard) to encrypt the pin-reset which would be sent along with the authentication data of the entity who conducted the transaction in order to allow the customer to ensure that the data received was sent by a specific entity (also in the previously cited column/line number). One would have been motivated to modify the method disclosed in Geer et al. with Kanevsky because doing so ensures that the information transmitted is both confidential and can only be decrypted by the user who has the private key associated with the public key of the smartcard.

Applicants also contend that "Geer or Kanevsky, taken individually or in combination, do not teach or suggest that a certificate and an associated private key is a plurality of certificates and associated private keys, wherein at least one of the certificates and private keys is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy." Examiner respectfully disagrees. Geer teaches that one of the plurality of certificates is a role certificate which is associated with a private key for communicating with other entities that are active in that role and wherein the role certificate includes at least one policy (col. 2, lines 51-60; col. 3, lines 29-33; and col. 5, lines 1-6). Furthermore, Geer teaches many other types of certificates that are used in the various embodiments disclosed.

Finally, Applicants contend that the cited combination of Geer, Kanevsky, and Burn does

not teach/suggest "decrypting a certificate and associated private key using a private key stored in the token requires the entry of a passphrase." Furthermore, Applicants contend that in the given combination the references teach away from one another because Kanevsky's reset takes place when a user forgets the PIN. With regards to Kanevsky, the Examiner would like to point out that Kanevsky teaches that there are several reasons why one would need a PIN reset (not just in the case that the user forgot his/her PIN) in col. 8, lines 21-31. Thus, Kanevsky does not teach away from the claimed invention which requires a passphrase to decrypt. Finally, with regards to the claimed limitation that Applicants contend the cited combination does not teach or suggest, Burn teaches that the disclosed combination should be modified to require a passphrase to access the smartcard's functions, such as decryption, since Burns requires the user to enter a PIN before allowing decryption which is implemented by using the certificate's data/functions (as seen in fig. 5, elements 140 and 150). The modification is motivated by Burn to allow for increased security and access control so that only the authorized entity may view the contents of the smartcard/data held therein (par. 6).

Due to the reasons stated above, the Examiner maintains rejections with respect to claims 1-16. Geer teaches the limitations that the Applicant suggests distinguish from the prior art. Furthermore, Kanevsky and Burn in combination with Geer teach the limitations not explicitly disclosed by Geer. Therefore, it is the Examiner's conclusion that the claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-6, 8-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr. et al., United States Patent No. 6,192,131, and further in view of Kanevsky et al., United States Patent No. 6,615,171.

As per claims 1 and 9:

Geer, Jr. et al. teach a method comprising: accessing the token through a token reader connected to a computer system by a certificate authority (col. 2, lines 27-39); reading a user signature certificate from the token (col. 2, lines 51-60); creating a certificate and an associated private key and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority (col. 9, lines 24-41); downloading the certificate and the associated private key to the token (col. 6, lines 15-27); and decrypting the certificate and the associated private key to the token, such that the token stores at least the private key, the user signature certificate and the certificate and the associated private key (col. 4, lines 15-25 and col. 6, lines 15-27).

Not explicitly disclosed is reading a token ID and searching for a match for the token ID and the signature certificate in an authoritative database and wherein the certificate and the associated private key are wrapped with a public key associated with the token ID if a match for the token ID and the user signature certificate is found in the authoritative database. However, Kanevsky et al. teach that the token ID and certificate as supplied by the user's smart card are searched for in a database to determine whether or not a valid user is attempting to gain access to

the system. Furthermore, Kanevsky et al. teach that once a user is identified as being valid, the encryption can occur. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Geer, Jr. et al. to incorporate the ability to determine that the users are who they say they are by checking a database for the token ID and certificate information supplied by the users' smart card and to allow other steps, such as for encryption to occur only when a match is found. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Kanevsky et al. suggest that searching for a match in the database allows one to verify that the user is a valid user to ensure that only valid users ultimately gain access to the resources such as the ability to encrypt the data at hand in col. 8, lines 29-46.

As per claims 2 and 10:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 1 and 9 above. Furthermore, Geer, Jr. et al. teach the method, wherein the certificate and the associated private key is a plurality of certificates and associated private keys wherein at least one of the plurality of certificates and associated private keys is a signature certificate for the user, an encryption certificate and associated private key for the user and a role certificate and associated private key for the user wherein the role certificate includes at least one policy (col. 2, lines 51-60 and col.3, lines 29-33).

As per claim 3 and 11:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 2 and 10 above. Furthermore, Geer, Jr. et al. teach the method wherein the wrapping of the certificate and the associated private key with the public key of the token encrypts the certificate and the

associated private key (col. 3, lines 16-22).

As per claims 4 and 12:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 3 and 11 above. Furthermore, Geer, Jr. et al. teach the method, wherein the token is a smart card (col. 2, lines 27-36).

As per claims 5 and 13:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 4 and 12 above. Furthermore, Kanevsky et al. teach the method wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user (col. 7, lines 49-59).

As per claims 6 and 14:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 5 and 13 above. Furthermore, Geer, Jr. et al. teach the method wherein downloading the certificate and the associated private key to the token is done through an unsecured communications line (col. 11, lines 50-59).

As per claims 8 and 16:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 1 and 9 above. Furthermore, Geer, Jr. et al. teach the method further comprising: authenticating, by the signing of the certificate and associated private key using a signature certificate of the certificate authority, that the certificate and associated private key were issued by the certificate authority (col. 4, lines 4-9).

III. Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geer, Jr.

et al., United States Patent No. 6,192,131 and Kanevsky et al., United States Patent No. 6,615,171 as applied to claims 7 and 15 above, and further in view of Burn, United States Pub. No: 2003/0005291.

As per claims 7 and 15:

Geer, Jr. et al. and Kanevsky et al. substantially teach the method recited in claims 6 and 14 above. Not explicitly disclosed is wherein decrypting the certificate and associated private key using the private key stored in the token requires the entry of a pass phrase by a user. However, Burn teaches the method of having a user PIN in order to access the certificate which is what allows access to decrypt messages received, the first of which contains the certificate of the server (fig. 5, elements 140 and 150). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Geer, Jr. et al. to incorporate the ability to check for a pass phrase entered by the user to allow the decryption to occur. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Burn suggests that adding the step of a user entering a pass phrase ensures that only the user can gain access to the securely encrypted materials so as not to compromise the data on the token in par. 6.

References Cited, Not Used

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. U.S. Patent No. 6,003,014
2. U.S. Patent No. 6,460,138
3. U.S. Patent No. 5,721,781
4. U.S. Patent No. 5,671,279
5. U.S. Pub. No. 2002/0026578
6. U.S. Pub. No. 2001/0002485

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
10/2/2006

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER